Feuille 1 : éléments de correction

Ex1 q1) Il s'agit de $1, 2, 4, 5, 10, 20, 25, 50, 100$ car $100 = 2^2 \cdot 5^2$ donc si $d \mid 100$ alors $d = 2^i 5^j$ avec $0 \leq i \leq 2$, $0 \leq j \leq 2$

et $1 = 2^0 \cdot 5^0$, $2 = 2^1 \cdot 5^0$, $4 = 2^2 \cdot 5^0$, $5 = 2^0 \cdot 5^1$, $10 = 2^1 \cdot 5^1$, $20 = 2^2 \cdot 5^1$, $25 = 2^0 \cdot 5^2$, $50 = 2 \cdot 5^2$, $100 = 2^2 \cdot 5^2$ sont les 9 diviseurs possibles.

q2) On a $6\,000\,000 = 6 \cdot 10^6 = 3 \cdot 2^7 \cdot 5^6 = 2^7 \cdot 3 \cdot 5^6$ donc si $d \mid 6000000$ alors $d = 2^\alpha 3^\beta 5^\gamma$ avec

$0 \leq \alpha \leq 7 \rightsquigarrow 8$ possibilités

$0 \leq \beta \leq 1 \rightsquigarrow 2$ possibilités

$0 \leq \gamma \leq 6 \rightsquigarrow 7$ possibilités

Par conséquent $6\,000\,000$ admet $8 \cdot 2 \cdot 7 = 112$ diviseurs positifs.

q3) La décomposition en facteurs premiers de $13! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13$ est $13! = 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$ donc d'après le raisonnement des deux premières questions $13!$ admet $11 \cdot 6 \cdot 3 \cdot 2 \cdot 2 \cdot 2 = 1584$ diviseurs positifs.

Si on veut compter aussi les diviseurs négatifs, il suffit d'en prendre deux fois plus, càd 3168 diviseurs positifs ou négatifs.

Ex2 On a $105 = 7 \cdot 15$ et $994 = 7 \cdot 142$ et si $101 < n < 1001$ et $n = 7k$ alors $7 \cdot 15 \leq n = 7k \leq 7 \cdot 142$ avec $15 \leq k \leq 142$.

Puisque k peut prendre $142 - 14 = 128$ valeurs, il y a 128 entiers divisibles par 7, strictement compris entre 101 et 1001.

On aurait pu dire aussi $14 = \left[\frac{101}{7}\right] < k < \left[\frac{1001}{7}\right] = 143$.

Ex3 Si on note a et b les deux nombres il s'agit de résoudre

$$\begin{cases} a = 538 + b \\ a = 13b + 22 \end{cases} \quad \text{ou} \quad \begin{cases} a = 538 + b \\ b = 13a + 22 \end{cases}$$

. Le premier système devient $12b = 516$ donc $\begin{cases} b = 43 \\ a = 581 \end{cases}$. Le second devient $-12a = 560$ qui n'a pas de solutions en nombres entiers car 3 ne divise pas 560.

Ex4 On a $2k+1 = 4q + r$ avec $0 \leq r < 4$. Comme $4q + r$ est impair, on exclut les cas $r = 0$ ou $r = 2$, ce qui nous laisse les possibilités $r = 1$ ou $r = 3$, qui peuvent arriver toutes les deux, par exemple pour $2k+1 = 5 = 4 \cdot 1 + 1$ ou pour $2k+1 = 7 = 4 \cdot 1 + 3$.

On a donc $(2k+1)^2 = (4q+1)^2 = 16q^2+8q+1 = 8(2q^2+q)+1$

ou bien $(2k+1)^2 = (4q+3)^2 = 16q^2+24q+9 = 8(2q^2+3q+1)+1$

ce qui signifie exactement que le reste de la division euclidienne de $(2k+1)^2$ par 8 est toujours 1.

On aurait pu se convaincre de cela aussi en élevant directement $(2k+1)^2 = 4k^2+4k+1 = 4k(k+1)+1$ et en remarquant que $k(k+1) = 2l$ est un entier pair en tant que produit de deux entiers consécutifs.

$\boxed{Ex5}$ q1) On a $\boxed{b = ka}$ et $\boxed{c = lb}$ donc $c = lka$ donc $a|c$.

q2) On a $\boxed{b = ka}$ et $\boxed{c = la}$ donc $2b+3c = 2ka+3la = a(2k+3l)$

c-à-d $a|c$.

q3) On a $\boxed{b = ka}$ et $\boxed{c = la}$ donc $c^2-2b = l^2a^2-2ka = a(l^2a-2k)$

d'où $a|c$.

q4) cette affirmation est fausse car par exemple si a et b sont premiers entre eux, d'après le théorème de Bezout, $\exists\, \alpha$ et $\beta \in \mathbb{Z}$ tels que $1 = \alpha a + \beta b$. En multipliant par 4 cette égalité on a $4 = 4\alpha a + 4\beta b$ avec $u = 4\alpha$ et $v = 4\beta$ entiers, sans que pgcd(a,b) soit égal à 4. Exemple numérique $a = b = 1$, $\alpha = 2, \beta = -1$, $u = 8, \beta = -4$. On a bien $8 \cdot 1 - 4 \cdot 1 = 4$ et pgcd$(1,1) = 1 \neq 4$.

q5) Si pgcd$(a, b^3) \neq 1$, il existe un premier p tel que $p|a$ et $p|b^3$. Alors p est un facteur premier de b^3, qui a les mêmes facteurs premiers que b. Donc $p|b$, Par conséquent $p\,|$ pgcd$(a,b) = 1$ ce qui contredit notre hypothèse de départ. En conclusion pgcd$(a, b^3) = 1$ et l'affirmation est vraie.

q6) Cette affirmation est fausse car si b et c sont impairs, on a bien pour $a=2$ que $2|b+c$ et $2|b-c$ sans que $2|b$ ou $2|c$.

<u>Exemple numérique</u> : $a=2$, $b=c=1$.

q7) Si $p|a$ et $p|b$ alors $p\,|\,7a-9b = 1$ donc $p = \pm 1$ ce qui signifie bien que pgcd$(a,b) = 1$, donc que a et b sont premiers entre eux

$\boxed{ex5.}$ q8) On doit avoir $b = ka$, $c = lb$ et $a = sc = slb = slka$ avec $s, l, k \in \mathbb{Z}$. Par conséquent $a(1 - slk) = 0$. Si $a = 0$ alors $b = c = 0$ et $|a| = |b|$. Si $a \neq 0$ alors $1 = slk$ donc $k = \pm 1$ càd encore $|a| = |b|$.

q9) Puisque 19 est premier, et $19 | ab$, c'est que 19 apparaît comme facteur premier de $a \cdot b$. Par conséquent 19 est facteur premier de a ou de b donc $19 | a$ ou $19 | b$.

q10) On peut écrire $a = kb$ et $c = ld$ ce qui donne $a + c = kb + ld$ sans pouvoir conclure à une égalité $a + c = s(b + d)$. En effet cette affirmation est fausse. Exemple numérique : $a = b = d = 1$, $c = 2$ et $a + c = 3$ n'est pas multiple de $b + d = 2$.

q11) On a $\text{pgcd}(a, b)\,\text{ppcm}(a, b) = |ab|$ car si $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ et $b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$ sont (pour $0 \leq \alpha_i$ et $0 \leq \beta_i$)

les décompositions en produits de facteurs premiers (distincts) de a et b on sait que
$$\text{pgcd}(a, b) = \prod_{i=1}^{s} p_i^{\min(\alpha_i, \beta_i)}$$
$$\text{ppcm}(a, b) = \prod_{i=1}^{s} p_i^{\max(\alpha_i, \beta_i)}$$

Or $\alpha_i + \beta_i = \min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i)$ d'où l'égalité annoncée.

Par conséquent $\text{ppcm}(a, b) = |ab|$ ssi $\text{pgcd}(a, b) = 1$ ssi a et b sont premiers entre eux.

q12) En effet si $c = ka$ et $d = lb$, on a $cd = klab$ donc $ab | cd$.

q13) Cette affirmation est fausse car 9 n'est pas premier donc on peut avoir $3 | a$ et $3 | b$ donc $9 | ab$ sans que 9 divise b.

Exemple numérique $a = b = 3$.

q14) Si $b = ka$ on a $bc = kac$ donc $a | bc$.

Si $c = la$ on a $bc = lab$ donc $a | bc$.

q15) Si a divise b alors $|b|$ est un multiple de a et de b.

Si c est un multiple de a et de b alors c est un multiple de $|b|$ donc $\text{ppcm}(a, b) = |b|$ (qui est par définition le plus petit commun multiple positif de a et de b)

Si $\text{ppcm}(a, b) = |b|$ c'est que $a | |b|$ donc que $a | b$.

Donc l'affirmation est vraie.

q16) Si $a=\pm 1$ alors a divise b pour tout $b \in \mathbb{Z}$ tout en étant premier à b. Donc l'affirmation est fausse. En fait elle est équivalente à $\operatorname{pgcd}(a,b)=|a|$ et pour $|a|=1$, a est premier à b.

q17) Cette affirmation est fausse car on peut avoir par exemple $a=4$, $b=6$, $\operatorname{pgcd}(a,b)=2\neq 1$ et $4\nmid 6$ et $6\nmid 4$.

q18) En effet si b et c sont pairs, alors $2|b$ et $2|c$ donc $b=2b'$, $c=2c'$, d'où $bc=4b'c'$ c-à-d $4|bc$.

Par conséquent si $4\nmid bc$ on doit avoir b ou c impair.

q19) Cette affirmation est fausse car par exemple si $a=2$, $b=4$ et $c=2$ on a bien $a|b$, $b\nmid c$ et $a|c$.

q20) Si $5|b^2$ alors $5|b$ car 5 est premier (et un facteur premier de b^2 est un facteur premier de b). Alors $b=5b'$ donc $b^2=25b'^2$ d'où $25|b^2$.

q21) Si $12=2^2.3$ divise b^2 alors $2|b^2$ et $3|b^2$ donc $6|b^2$ or $4|b^2$ $9|b^2$ mais on ne peut pas conclure que $4|b$. En effet l'affirmation est fausse en prenant par exemple $b=6$.

q22) D'après q21) on a $2|b^2$ et $3|b^2$ donc $2|b$ et $3|b$. Puisque 2 et 3 sont premiers entre eux on a que $6|b$ (2 et 3 sont facteurs premiers de b). Donc $b=6b'$, d'où $b^2=36b'^2$ et $36|b^2$.

q23) On a $91=7.13$ donc 91 n'est pas premier. Pour $a=7$, $b=13$ on a bien $91|ab$ sans que 91 divise a ou 91 divise b.
Cette affirmation est donc fausse.

$\boxed{\text{Ex 6}}$ q1) Le produit de deux nombres consécutifs est divisible par 2 car l'un d'eux est forcément pair. Le produit P de trois nombres consécutifs est divisible par 3 car l'un des trois nombres est forcément un multiple de 3. Comme $2|P$ et $3|P$ et que $\operatorname{pgcd}(2,3)=1$ on a $6|P$. On peut dire aussi que 2 et 3 sont facteurs premiers de P.

q2) Si Q est le produit de quatre nombres consécutifs on a $3|Q$ d'après la q1). Parmi les quatre nombres il y en a un qui est divisible par 4 et un autre qui est divisible par 2 (différent de celui qui est divisible par 4). Le produit de ces deux nombres est divisible par 8 donc $8|Q$. Comme $\operatorname{pgcd}(3,8)=1$ on a $3.8=24$ qui divise Q.

ex 7 Pour $n = 8 = 2^3$ ~~on~~ a $2^3 \mid m^2$ et comme la décomposition de m^2 en facteurs premiers comporte que des puissances paires, on doit avoir $2^4 \mid m^2$. Le plus petit $m > 0$ tel que $16 \mid m^2$ est donc $m = 4$.

Pour $n = 16$ on a de nouveau $m = 4$ car $n = 4^2$.

Pour $n = 6$ on a $6 \mid m^2$ donc $36 \mid m^2$ d'où $m = 6$.

Pour $n = 12$ on a $12 \mid m^2$ donc $36 \mid m^2$ d'où $m = 6$.

Pour $n = 30$ on a $2 \cdot 3 \cdot 5 \mid m^2$ donc $900 \mid m^2$ d'où $m = 30$.

Pour $n = 90$ on a $2 \cdot 3^2 \cdot 5 \mid m^2$ donc $900 \mid m^2$ d'où $m = 30$.

Pour $n = 98$ on a $2 \cdot 7^2 \mid m^2$ donc $196 \mid m^2$ d'où $m = 14$

Pour $n = 72$ on a $2^3 \cdot 3^2 \mid m^2$ donc $144 \mid m^2$ d'où $m = 12$.

Pour $n = 8100$ on a $90^2 \mid m^2$ donc $m = 90$.

Pour $n = 900$ on a $30^2 \mid m^2$ donc $m = 30$.

ex 8 On effectue des divisions successives par 7 :

$$
\begin{array}{r|l}
2017 & 7 \\
-14 & 288 \\
61 & \\
-56 & \\
57 & \\
-56 & \\
1 &
\end{array}
\qquad
\begin{array}{r|l}
288 & 7 \\
-28 & 41 \\
8 & \\
7 & \\
1 &
\end{array}
\qquad
\begin{array}{r|l}
41 & 7 \\
35 & 5 \\
6 &
\end{array}
$$

Donc
$$2017 = 7 \cdot 288 + 1 =$$
$$= 7 \cdot (7 \cdot 41 + 1) + 1 =$$
$$= 7(7 \cdot (7 \cdot 5 + 6) + 1) + 1$$
$$= 7^3 \cdot 5 + 7^2 \cdot 6 + 7 \cdot 1 + 1$$

Cela signifie que $2017_{10} = 5611_7$. On voit que cela revient à reprendre dans l'ordre inverse le quotient final et les restes obtenus.

ex 9
$$n = 512121_9 = 5 \cdot 9^5 + 1 \cdot 9^4 + 2 \cdot 9^3 + 1 \cdot 9^2 + 2 \cdot 9 + 1 =$$
$$= 5 \cdot 59049 + 1 \cdot 6561 + 2 \cdot 729 + 1 \cdot 81 + 2 \cdot 9 + 1 =$$
$$= 295245 + 6561 + 1458 + 81 + 18 + 1 =$$
$$= 303364_{10}$$

ex 10
$$713_8 = 7 \cdot 8^2 + 1 \cdot 8 + 3 = 7 \cdot 64 + 11 = 459_{10} = 1224_7$$

$$
\begin{array}{r|l}
459 & 7 \\
42 & 65 \\
39 & \\
35 & \\
4 &
\end{array}
\qquad
\begin{array}{r|l}
65 & 7 \\
63 & 9 \\
2 &
\end{array}
\qquad
\begin{array}{r|l}
9 & 7 \\
7 & 1 \\
2 &
\end{array}
$$

car $459 = 7 \cdot 65 + 4 = 7 \cdot (7 \cdot 9 + 2) + 4 =$
$$= 7^2 \cdot 9 + 7 \cdot 2 + 4$$

ex. 11 q1) $10! = 1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8\cdot9\cdot10 =$

$$= 2\cdot3\cdot2^2\cdot5\cdot(2\cdot3)\cdot7\cdot2^3\cdot3^2\cdot(2\cdot5)$$
$$= 2^8\cdot3^4\cdot5^2\cdot7$$

q2)

Dans le produit $1\cdot2\cdot3\cdot4\cdot \quad \cdot100 = 100!$ il y a d'abord une contribution de 1 pour chaque nombre pair dans $\nu_2(100!)$ = la plus grande puissance de 2 qui divise $100!$

(On note $\nu_p(n)$ la plus grande puissance de p qui divise n)

Donc, comme il y a $\frac{100}{2} = 50$ nombres pairs de 1 à 100

on a $\nu_2(100!) = 50 + \nu_2(50!)$

En effet, ~~on~~ en divisant par 2 chacun de ces nombres pairs pour enlever cette contribution on doit s'occuper maintenant de

$$\nu_2(50!) = \nu_2\left(\frac{2}{2}\cdot\frac{4}{2}\cdot\frac{6}{2}\cdot \quad \cdot\frac{100}{2}\right) = \nu_2(1\cdot2\cdot3 \cdot \quad \cdot50)$$

On répète le procédé ci-dessus : il y a $\frac{50}{2} = 25$ nombres pairs de 1 à 50 qui apporte chacun une contribution de 1 dans $\nu_2(50!)$, qui sera donc $\nu_2(50!) = 25 + \nu_2(25!)$ car

$$\frac{2}{2}\cdot\frac{4}{2}\cdot\frac{6}{2}\cdot \quad \cdot\frac{50}{2} = 1\cdot2\cdot\cdot \quad \cdot25 = 25!$$

On continue de la même manière $\nu_2(100!) = \left[\frac{100}{2}\right] + \left[\frac{50}{2}\right] + \left[\frac{25}{2}\right] + \nu_2(12!)$

car $\nu_2(25!) = \nu_2(24!) = 12 + \nu_2\left(\frac{2}{2}\cdot\frac{4}{2}\cdot \quad \cdot\frac{24}{2}\right)$ et ainsi de suite

$$\nu_2(12!) = \left[\frac{12}{2}\right] + \nu_2(6!) = \left[\frac{12}{2}\right] + \left[\frac{6}{2}\right] + \nu_2(3!) = 6+3+1$$

Finalement $\nu_2(100!) = \left[\frac{100}{2}\right] + \left[\frac{50}{2}\right] + \left[\frac{25}{2}\right] + \left[\frac{12}{2}\right] + \left[\frac{6}{2}\right] + \left[\frac{3}{2}\right] = 97$

et on comprend que cette formule se généralise à

$$\nu_2(n!) = \left[\frac{n}{2}\right] + \left[\frac{\left[\frac{n}{2}\right]}{2}\right] + \left[\frac{\left[\frac{\left[\frac{n}{2}\right]}{2}\right]}{2}\right] + \cdots$$

Pour simplifier la formule montrons que $\left[\frac{\left[\frac{n}{p}\right]}{p}\right] = \left[\frac{n}{p^2}\right]$

Écrivons pour cela la division euclidienne de n par p :

$n = q_1 \cdot p + r_1$ avec $0 \leq r_1 \leq p-1$ et ensuite la

division euclidienne de q_1 par p :

$q_1 = q_2 \cdot p + r_2$ avec $0 \leq r_2 \leq p-1$.

Alors $n = q_1 p + r_1 = p(p q_2 + r_2) + r_1 = p^2 q_2 + p r_2 + r_1$

avec
$$\begin{array}{l} 0 \leq p r_2 \leq p(p-1) \\ 0 \leq r_1 \leq p-1 \\ \hline 0 \leq p r_2 + r_1 \leq (p+1)(p-1) = p^2 - 1 \end{array}$$

Donc $n = p^2 q_2 + (p r_2 + r_1)$ est la division euclidienne de n par p^2. Or $\left[\frac{n}{p}\right] = q_1$, $\left[\frac{\left[\frac{n}{p}\right]}{p}\right] = \left[\frac{q_1}{p}\right] = q_2$

et $\left[\frac{n}{p^2}\right] = q_2$ d'où l'égalité.

La formule recherchée est donc

$$\nu_2(n!) = \left[\frac{n}{2}\right] + \left[\frac{n}{2^2}\right] + \left[\frac{n}{2^3}\right] + \cdots$$

qui se généralise encore à

$$\nu_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

<u>Cas particulier</u> : $n = 10$, $p = 2$ on a bien $\nu_2(10!) = \left[\frac{10}{2}\right] + \left[\frac{10}{4}\right] + \left[\frac{10}{8}\right]$
$= 8$

comme à la question 1

De même $n = 10$, $p = 3$ on a $\nu_3(10!) = \left[\frac{10}{3}\right] + \left[\frac{10}{9}\right] = 3 + 1 = 4$

$n = 10$, $p = 5$, $\nu_5(10!) = \left[\frac{10}{5}\right] = 2$

$n = 10$, $p = 7$, $\nu_7(10!) = \left[\frac{10}{7}\right] = 1$.

q3) Le nombre de zéros cherché est la puissance maximale de 10 dans la décomposition de $100!$, obtenue comme $\min(\nu_2(100!), \nu_5(100!))$ car $10 = 2 \cdot 5$ et $\nu_{10}(100!)$ tient compte de la puissance maximale du "couple" $2\cdot5$ dans la décomposition en facteurs premiers de $100!$.

On $\nu_2(100!)=97$ et $\nu_5(100!)=\left[\frac{100}{5}\right]+\left[\frac{100}{25}\right]=20+4=24$

Donc il y a 24 zeros à la fin de l'écriture décimale de $100!$ (on peut s'imaginer mieux ainsi l'ordre de grandeur de ce nombre, immense !).

---

ex 12 On a $M_n=2^{n-1}+\dots+2^2+2+1=\dfrac{2^n-1}{2-1}=2^n-1$

Par conséquent $M_n^2=2^{2n}-2^{n+1}+1=2^{2n-1}+2^{2n-1}-2^{n+1}+1=$

$=2^{2n-1}+2^{2n-2}+2^{2n-2}-2^{n+1}+1=2^{2n-1}+2^{2n-2}+\dots+2^{n+1}+2^{n+1}-2^{n+1}+1$

$=2^{2n-1}+2^{2n-2}+\dots+2^{n+1}+1=\underset{\uparrow\,2n}{1}11\dots\underset{\uparrow\,n+2}{1}00\dots0\underset{\uparrow\,1}{1}{}_2$

$=M_{2n}-M_{n+1}+M_1$

ex 13 Si $a=2^3\times3^5\times7^2$ et $b=2\times5^2\times7^3$ on a

$\mathrm{pgcd}(a,b)=2\times7^2$ et $\mathrm{ppcm}(a,b)=2^3\times3^5\times5^2\times7^3$.

ex 14 On a $210=2\times3\times5\times7$ et comme $\mathrm{pgcd}(n,210)=1$ on sait que la décomposition en facteurs premiers de n est
$n=11^{\alpha_1}\cdot13^{\alpha_2}\cdots97^{\alpha_{21}}$ avec $\alpha_i\geq0$. Or $11^2\geq100$

donc parmi $(\alpha_1,\dots,\alpha_{21})$ il n'y a qu'un seul α_i non nul, et cet α_i est au plus égal à 1. En effet, la présence d'un $\alpha_i\geq2$ entraîne $n\geq11^2>100$, et la présence de $\alpha_i=\alpha_j=1$ entraîne $n\geq11\cdot13>11^2>100$. Par conséquent n est premier compris entre 10 et 100 c.à.d $n\in\{11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97\}$.

ex 15 a1) Cette question a été vue en cours, avec une preuve qui utilisait l'algorithme d'Euclide. On peut en donner une qui utilise la décomposition de a,b,c en facteurs premiers. Écrivons à cet effet $a=\pm p_1^{\alpha_1}\cdots p_s^{\alpha_s}$, $b=\pm p_1^{\beta_1}\cdots p_s^{\beta_s}$, $c=\pm p_1^{\gamma_1}\cdots p_s^{\gamma_s}$

avec $\alpha_i,\beta_i,\gamma_i\geq0$ et $p_1,\dots,p_s$ les facteurs premiers distincts de a, b et c.

Par conséquent les décompositions de ca et cb sont

$$ca = \pm \prod_{i=1}^{s} p_i^{\alpha_i + \gamma_i}, \quad cb = \pm \prod_{i=1}^{s} p_i^{\beta_i + \gamma_i}$$, ce qui entraîne

$$\operatorname{pgcd}(ca, cb) = \prod_{i=1}^{s} p_i^{\min(\alpha_i + \gamma_i, \beta_i + \gamma_i)} = \prod_{i=1}^{s} p_i^{\gamma_i + \min(\alpha_i, \beta_i)}$$

car $\min(\alpha_i + \gamma_i, \beta_i + \gamma_i) = \gamma_i + \min(\alpha_i, \beta_i) \quad \forall i \in \{1, \ldots, s\}$.

En effet $\alpha_i + \gamma_i \leq \beta_i + \gamma_i$ ssi $\alpha_i \leq \beta_i$.

Alors $\operatorname{pgcd}(ca, cb) = \left(\prod_{i=1}^{s} p_i^{\gamma_i}\right) \operatorname{pgcd}(a, b) = |c| \operatorname{pgcd}(a, b)$.

q2) En gardant les mêmes notations on a $a^2 = \prod_{i=1}^{s} p_i^{2\alpha_i}$, $b^2 = \prod_{i=1}^{s} p_i^{2\beta_i}$

$$\operatorname{pgcd}(a^2, b^2) = \prod_{i=1}^{s} p_i^{\min(2\alpha_i, 2\beta_i)} = \prod_{i=1}^{s} p_i^{2\min(\alpha_i, \beta_i)}$$ car

($\alpha_i \leq \beta_i$ ssi $2\alpha_i \leq 2\beta_i$) donc $\min(2\alpha_i, 2\beta_i) = 2\min(\alpha_i, \beta_i)$.

Par conséquent $\operatorname{pgcd}(a^2, b^2) = \left(\prod_{i=1}^{s} p_i^{\min(\alpha_i, \beta_i)}\right)^2 = \operatorname{pgcd}(a, b)^2$.

q3) Si p est premier et $p | c$, $p | b$ alors $p | a$ et $p | b$ donc $p | \operatorname{pgcd}(a, b) = 1$

Ceci est impossible donc aucun premier ne divise b et c à la fois

d'où $\operatorname{pgcd}(b, c) = 1$.

q4) Si $\operatorname{pgcd}(a, bc) = 1$ alors d'après q3), vu que $b | bc$ et $c | bc$

on a $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(a, c) = 1$.

Si réciproquement $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(a, c) = 1$ et p est premier

tel que $p | a$ et $p | bc$ alors, d'après le lemme d'Euclide,

on a $p | b$ ou $p | c$. Or si $p | a$, $p | b$ on a $p | \operatorname{pgcd}(a, b) = 1$ d'où

une contradiction et si $p | a$, $p | c$ on a $p | \operatorname{pgcd}(a, c) = 1$, ce qui est

de nouveau contradictoire. Par conséquent aucun premier ne divise

a et bc à la fois ce qui signifie exactement que

$\operatorname{pgcd}(a, bc) = 1$.

q5) Si $d \mid a+b$ et $d \mid a-b$ alors $d \mid a+b+a-b=2a$ et $d \mid (a+b)-(a-b)=2b$
donc $d \mid \mathrm{pgcd}(2a,2b)=2\,\mathrm{pgcd}(a,b)=2$. Donc $d=\pm1$ ou $d=\pm2$ donc $\mathrm{pgcd}(a+b,a-b)=1$ ou 2 F 1, 10
(ex : $a=1$, $b=1$, $\mathrm{pgcd}(2,0)=2$ et $a=1$, $b=0$, $\mathrm{pgcd}(1,0)=1$). Si $p \mid a+b$ et $p \mid ab$ avec p premier
on a $p \mid a$ ou $p \mid b$. Donc $p \mid a+b-a=b$ ou $p \mid a+b-b=a$ donc $p \mid \mathrm{pgcd}(a,b)=1$.
Donc $\mathrm{pgcd}(a+b,ab)=1$

ex 16 Si $d \mid n$ et $d \mid n+1$

on a $d \mid n+1-n=1$ donc $d=\pm1$ donc $\mathrm{pgcd}(n,n+1)=1$.

Par conséquent $\mathrm{ppcm}(n,n+1)=\dfrac{n(n+1)}{\mathrm{pgcd}(n,n+1)}=n(n+1)$.

ex 17

q1) On a $637=7^2\times13$ et $595=5\times7\times17$ donc

$\mathrm{pgcd}(637,595)=7$.

On aurait pu effectuer aussi l'algorithme d'Euclide :

$637=595+42$

$595=42\times14+\boxed{7}$

$42=6\times7+0$ avec un dernier reste non nul égal à 7.

q2) On a $637x+595y=91=7\times13$. On peut donc dire que l'équation a des solutions, vu que $7 \mid 91$.

On doit, pour la seconde, trouver d'abord une solution particulière. Cette solution nous est fournie par des coefficients de Bezout soit pour 637 et 595 obtenus en remontant l'algorithme d'Euclide de la q1), soit pour $\frac{637}{7}=91$ et $\frac{595}{7}=85$ premiers entre eux, vu que notre équation est équivalente à l'équation $91x+85y=13$.

La première variante nous donne : $7=595-42\times14=$
$=595-(637-595)\times14=637\times(-14)+595\times15$

d'où $7\times13=637\times(-14\cdot13)+595\times(15\cdot13)$.

On pose $x_0=-14\cdot13$, $y_0=15\cdot13$ et on obtient

$637x+595y=637x_0+595y_0$ (=)

$637(x-x_0)=595(y_0-y)$. Cela ~~équivaut~~ à $91(x-x_0)=85(y_0-y)$

et comme $\mathrm{pgcd}(91,85)=1$ on a $91 \mid y_0-y$ par le lemme de Gauss. On écrit alors

$y_0-y=91k$, avec $k\in\mathbb{Z}$. L'équation $91(x-x_0)=85(y_0-y)$

devient $91(x-x_0)=85\cdot 91\cdot k \iff x-x_0=85k \iff$
$x=85k+x_0$.

Posons $x=85k+x_0$, $y=y_0-91k$ pour $k\in\mathbb{Z}$. Alors on a

bien $637(85k+x_0)+595(y_0-91k)=637x_0+595y_0=91$

Donc les solutions de l'equations sont effectivement

de la forme $x=85k+x_0=85k-14\cdot 13$

$y=y_0-91k=15\cdot 13-91k$ pour $k\in\mathbb{Z}$.

La deuxième variante consiste à écrire l'algorithme

d'Euclide pour 91 et 85, donc à diviser par 7 l'algorithme

d'Euclide de la q1) ; $91=85+6$

$85=6\times 14+\boxed{1}$

$6=6\times 1+0$ d'où

$1=85-6\times 14=85-(91-85)\times 14=85\cdot 15-91\cdot 14$

Posons $13=85\cdot\underbrace{13\cdot 15}_{y_0}+91\underbrace{(-13\cdot 14)}_{x_0}$ et $x_0=-13\cdot 14$, $y_0=13\cdot 15$

On a $13=91x+85y=91x_0+85y_0 \Rightarrow$

$91(x-x_0)=85(y_0-y)$. On arrive à la même situation

que ci-dessus donc aux mêmes solutions $\begin{cases} x=85k-14\cdot 13 \\ y=15\cdot 13-91k,\ k\in\mathbb{Z}\end{cases}$

q3) On a $143=11\cdot 13$ donc $7\nmid 143$. On sait alors que cette

équation n'a pas de solutions entières. En effet $7\mid 637x+595y$

si $x,y\in\mathbb{Z}$ donc $637x+595y\neq 143$.

Ex 18 q1) On a 283 premier et $1722=2\times 3\times 7\times 41$ donc

pgcd$(1722,283)=1$ et $1\mid 31$ donc cette équation

admet des solutions dans $\mathbb{Z}$. On doit trouver d'abord

une solution particulière, donc effectuer l'algorithme d'Euclide

entre 1722 et 283 pour trouver une relation de Bezout du type

$1722u+283v=1$.

On a $1722 = 283 \cdot 6 + 24$
$283 = 24 \cdot 11 + 19$
$24 = 19 + 5$
$19 = 5 \times 3 + 4$
$5 = 4 + 1$ d'où

$1 = 5 - 4 = 5 - (19 - 5 \times 3) = 5 \times 4 - 19 = (24 - 19) \times 4 - 19 =$

$= 24 \times 4 - 19 \times 5 = 24 \times 4 - (283 - 24 \cdot 11) \cdot 5 =$

$= 24 \cdot 59 - 283 \cdot 5 = (1722 - 283 \cdot 6) \cdot 59 - 283 \cdot 5 =$

$= 1722 \cdot 59 - 283 \cdot 359$ donc

$31 = 1722 \cdot \underbrace{59 \cdot 31}_{y_0} + 283 \underbrace{(-359 \cdot 31)}_{x_0}$ et on pose $x_0 = -359 \cdot 31$
$y_0 = 59 \cdot 31$
pour solution particulière.

On sait que $283x + 1722y = 283x_0 + 1722y_0$ (⇔)

$283(x - x_0) = 1722(y_0 - y)$ donc vu que

$\text{pgcd}(283, 1722) = 1$ on a $283 \mid y_0 - y$ d'après le lemme de Gauss. D'où $y = y_0 - 283k$ pour $k \in \mathbb{Z}$ et

$283(x - x_0) = 1722 \cdot 283 \cdot k$ (⇔) $x - x_0 = 1722k$

(⇔) $x = 1722k + x_0$.

On obtient toutes les solutions en prenant $x = 1722k - 359 \cdot 31$
$y = 59 \cdot 31 - 283k$
pour $k \in \mathbb{Z}$.

Q2) On a $365 = 73 \cdot 5$ et $72 = 2^3 \cdot 3^2$ donc $\text{pgcd}(365, 72) = 1$ et l'équation $365x + 72y = 18$ admet des solutions.

On écrit $365 = 72 \times 5 + 5$
$72 = 5 \times 14 + 2$
$5 = 2 \times 2 + 1$ donc $1 = 5 - 2 \times 2 = 5 - (72 - 5 \times 14) \times 2 =$

$= 5 \times 29 - 72 \times 2 = (365 - 72 \times 5) \times 29 - 72 \times 2 = 365 \times 29 - 72 \times 147$

et $18 = 365 \times \underbrace{29 \cdot 18}_{x_0} + 72 \underbrace{(-147 \cdot 18)}_{y_0} = 365x + 72y$. Alors

$365(x - x_0) = 72(y_0 - y)$ et comme $\text{pgcd}(365, 72) = 1$ on a

$y_0 - y = 365k$, $x - x_0 = 72k$, $k \in \mathbb{Z}$. Les solutions sont $x = 72k + 29 \cdot 18$
$y = -147 \cdot 18 - 365k$
$k \in \mathbb{Z}$.

93) On a 101 premier et $150 = 2 \times 3 \times 5^2$ donc $\mathrm{pgcd}(101,150) = 1$ et l'équation admet des solutions.

On écrit $150 = 101 \times 1 + 49$

$101 = 49 \times 2 + 3$

$49 = 3 \times 16 + 1$ donc $1 = 49 - 3 \times 16 = 49 - (101 - 49 \times 2) \times 16 =$

$= 49 \times 33 - 101 \times 16 = (150 - 101) \times 33 - 101 \times 16 = 150 \times 33 - 101 \cdot 49$

Alors $15 = 101\underbrace{(-49 \cdot 15)}_{x_0} + 150 \cdot \underbrace{33 \cdot 15}_{y_0} = 101x + 150y$ entraîne

$101(x - x_0) = 150(y_0 - y)$ et comme $\mathrm{pgcd}(101, 150) = 1$ on a

$y_0 - y = 101k$ et $x - x_0 = 150k$ pour $k \in \mathbb{Z}$.

Les solutions sont $x = 150k - 49 \cdot 15$

$y = 33 \cdot 15 - 101k$ pour $k \in \mathbb{Z}$.

94) On a $282 = 2 \times 3 \times 47$ et $678 = 2 \times 3 \times 113$ donc $\mathrm{pgcd}(282, 678) = 6$. Comme $6 \mid 66$ l'équation a des solutions.

Elle équivaut à $47x + 113y = 11$. On écrit

$113 = 47 \times 2 + 19$

$47 = 19 \times 2 + 9$

$19 = 9 \times 2 + 1$ donc $1 = 19 - 9 \times 2 = 19 - (47 - 19 \times 2) \times 2 =$

$= 19 \times 5 - 47 \times 2 = (113 - 47 \times 2) \times 5 - 47 \times 2 = 113 \times 5 - 47 \times 12$

d'où $11 = 47\underbrace{(-12 \cdot 11)}_{x_0} + 113\underbrace{(5 \cdot 11)}_{y_0} = 47x + 113y$. Comme $47(x - x_0) = 113(y_0 - y)$

et que $\mathrm{pgcd}(47, 113) = 1$ on a $y_0 - y = 47k$

$x - x_0 = 113k$ pour $k \in \mathbb{Z}$ donc les solutions

recherchées sont $x = 113k - 12 \cdot 11 = 113k - 132$

$y = 55 - 47k$, $k \in \mathbb{Z}$.

ex 19 Si $\mathrm{pgcd}(a, b) = 12$ on a que $a = 12a'$, $b = 12b'$ avec $\mathrm{pgcd}(a', b') = 1$. Alors $\mathrm{ppcm}(a, b) = 12a'b' = 360$

donc $a'b' = 30$. Par conséquent $(a', b') \in \{(1,30), (2,15), (3,10), (5,6), (6,5), (10,3), (15,2), (30,1)\}$ et $(a,b) \in \{(12, 360), (24, 180), (36, 120), (60, 72), (72, 60), (120, 36), (180, 24), (360, 12)\}$.

ex 20) a) On a que $a = 9a'$
$b = 9b'$ avec $pgcd(a', b') = 1$ et

$9(a'+b') = 360$ donc $a'+b' = 40$.

Par conséquent $(a', b') \in \{(1,39), (3,37), (7,33), (9,31), (11,29), (13,27),$
$(17,23), (19,21), (21,19), (23,17), (27,13), (29,11), (31,9), (33,7), (37,3), (39,1)\}$

et $(a,b) = 9(a', b') = (9a', 9b')$.

b) Si $a = 18a'$
$b = 18b'$ avec $pgcd(a', b') = 1$ on a $18^2 a'b' = 1620 = 18^2 \cdot 5$

donc $a'b' = 5$ et $(a', b') \in \{(1,5), (5,1)\}$ donc $(a,b) \in \{(18,90), (90,18)\}$

ex 21) q1) On a $16 = 7 \times 2 + 2$
$7 = 2 \times 3 + 1$ donc $1 = 7 - 2\times 3 = 7 - (16 - 7\times 2)\times 3 =$

$= 7\times 7 - 16\times 3 = 7\times 7 + 16(-3)$ et on peut prendre pour

solution particulière $x_0 = 7$, $y_0 = -3$.

q2) On a $7x_0 + 16y_0 = 7x + 16y \iff 7(x - x_0) = 16(y_0 - y)$.

Comme $pgcd(7,16) = 1$ cela entraine $y_0 - y = 7k$
$x - x_0 = 16k$ pour $k \in \mathbb{Z}$

donc les solutions recherchés sont $x = 16k + 7$
$y = -3 - 7k$ pour $k \in \mathbb{Z}$

q3) a) Si Alice possède un grand récipient en plus de ses deux récipient, elle peut juste mettre 7 fois 7 l dans ce grand récipient, et ensuite elle verse 3 fois 16 l ~~dans~~ 49 l du grand récipient pour arriver à 1 l car $7\times 7 - 16\cdot 3 = 1$.
Le problème ne suppose pas l'existence d'un grand récipient donc on va imiter cette procédure sans utiliser de grand récipient mais en remplissant 7 fois le récipient de 7 l et en le vidant petit à petit dans le récipient de 16 l (qui sera vidé 3 fois) pour aboutir à 1 l.

On fait un tableau qui montre les étapes successives de notre procédé :

Volume de liquide dans le récipient de 16 l à chaque étape	0	7	7	14	14	16	0	5	5	12	12	16	0	3	3	10	10	16
Volume de liquide dans le récipient de 7 l à chaque étape	7	0	7	0	7	5	5	0	7	0	7	3	3	0	7	0	7	1

On a utilisé 49 l d'eau et le récipient de 16 l a été rempli 3 fois (et vidé 2 fois)

On peut aussi utiliser la solution pour $k=-1$, qui correspond à $x=-9$, $y=4$ et à la formule $16\cdot 4 - 7\cdot 9 = 1$ et au tableau

Volume de liquide dans le récipient de 16 l	16	9	9	2	2	0	16	11	11	4	4	0	16	13	13	6	6	0	16	15	15	8
Volume de liquide dans le récipient de 7 l	0	7	0	7	0	2	2	2	0	7	0	4	4	7	0	7	0	6	6	7	0	7

8	1
0	7

On a utilisé $16\times 4 = 64$ l d'eau et le récipient de 16 l a été rempli 4 fois

b) On cherche donc une solution de l'équation avec y minimal en valeur absolue. Puisque $y=-7k-3$ cette solution correspond à $k=0$, $y=-3$ qui a été décrite ci-dessus.

Q4) Alice ne peut pas obtenir 1 l d'eau avec des récipients de 14 l et de 21 l car à chaque opération elle obtient une quantité de liquide qui correspond à α l avec α multiple de 7 ! En effet $\alpha = 21x + 14y$ est toujours un multiple de 7 pour $x, y \in \mathbb{Z}$.

ex22 Considérons

$\alpha_1 = (n+1)!+2$, $\alpha_2 = (n+1)!+3$, ..., $\alpha_n = (n+1)!+(n+1)$ pour $n \geqslant 1$

On a $2 \mid \alpha_1$, $3 \mid \alpha_2$, ..., $n+1 \mid \alpha_n$ et $\alpha_n = (n+1)\left(n!+1\right) > n+1$

En général $\alpha_i = (i+1)\left[\frac{(n+1)!}{i+1}+1\right] > i+1$ pour $1 \leqslant i \leqslant n$ donc α_i n'est pas premier.

ex23 On écrit $11p+1 = k^2$ pour $k \in \mathbb{Z}$. Les restes de k modulo 11 ne peuvent être que $0, \pm1, \pm2, \pm3, \pm4$ ou ±5 et pour chacun de ces cas les restes de k^2 modulo 11 sont $0, 1, 4, 9, 5$ ou 3. Par conséquent, pour que $k^2 = 11p+1$ on a nécessairement $k = 11k' \pm 1$ et $k^2 = 121k'^2 \pm 22k' + 1$ avec $k' \in \mathbb{Z}$. Alors $11p = 121k'^2 \pm 22k'$ $\Leftrightarrow$ $p = 11k'^2 \pm 2k' = k'(11k' \pm 2)$

Vu que p est premier et que $11k' \pm 2 \neq \pm 1$ on doit avoir $k' = \pm 1$

Pour $k' = -1$ on a $k = -12$ ou $k = -10$ donc $p = 13$ qui convient ou $p = 9$ qui ne convient pas.

Pour $k' = 1$ on a $k = 12$ ou $k = 10$ donc toujours $p = 13$ premier ou $p = 9$ qui n'est pas premier. La seule possibilité avec p premier est par conséquent $p = 13$

ex24. Puisque a et b sont premiers entre eux, leurs décompositions en facteurs premiers sont $a = \pm p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ $b = \pm p_{s+1}^{\alpha_{s+1}} \cdots p_t^{\alpha_t}$ avec $\alpha_i > 0$ et $p_1, \ldots, p_t$ des premiers distincts.

Par conséquent la décomposition en facteurs premiers de $ab = c^2$ est $p_1^{\alpha_1} \cdots p_s^{\alpha_s} p_{s+1}^{\alpha_{s+1}} \cdots p_t^{\alpha_t}$ et a et b sont de même signe.

Comme il s'agit de la décomposition en facteurs premiers d'un carré, on a $\alpha_i = 2\gamma_i$ pour tout i compris entre 1 et t.

On conclut facilement que $a = \pm p_1^{2\gamma_1} \cdots p_s^{2\gamma_s}$ et

$b = \pm p_{s+1}^{2\gamma_{s+1}} \cdots p_t^{2\gamma_t}$ sont des carrés au signe près.

ex25 On a $b \geqslant 2$ et $10101_b = b^4 + b^2 + 1 = b^4 + 2b^2 + 1 - b^2 = (b^2+1)^2 - b^2 = (b^2+b+1)(b^2-b+1)$. Ces deux facteurs étant strictement supérieurs à 1 on a bien que 10101_b n'est pas un nombre premier.

ex26 Les restes de $n \in \mathbb{N}$ modulo 7 sont $0, \pm 1, \pm 2$ ou ± 3 donc les restes de n^2 modulo 7 sont 0, 1, 4 ou 2 et les restes de n^3 modulo 7 sont $0, \pm 1, \pm 1$ ou ± 1. Si n est à la fois un carré et un cube, ses restes modulo 7 ne peuvent être que 0 ou 1 donc $\exists\, k \in \mathbb{N}$ tel que $n = 7k$ ou $7k+1$.

Voir la remarque après l'exercice 27 pour une autre solution.

ex27 q1) On écrit

$$25 = 9 \times 2 + 7$$
$$9 = 7 \times 1 + 2$$
$$7 = 2 \times 3 + 1$$

donc

$$1 = 7 - 2\times 3 = 7 - (9-7)\times 3 = 7\times 4 - 9\times 3 = (25 - 9\times 2)\times 4 - 9 \times 3 = 25 \times 4 - 9 \times 11$$

et on peut considérer $u = 4$, $v = -11$.

q2) On a $c^{25} = a^{25u} b^{25v} = a^{1-9v} (b^{25})^{v} = a \cdot a^{-9v} a^{9v} = a$ et

$c^{9} = a^{9u} b^{9v} = b^{25u + 9v} = b$

q3) Écrivons x sous forme de fraction simplifiée, $x = \frac{s}{t}$ avec $s, t \in \mathbb{Z}$ $\mathrm{pgcd}(s,t) = 1$. Alors si $x^k = \frac{s^k}{t^k} = m \in \mathbb{Z}$ on a $m t^k = s^k$. Si $t \neq \pm 1$ alors soit p un facteur premier de t. On a $p \mid s^k$ donc $p \mid s$ par le lemme d'Euclide, or $\mathrm{pgcd}(s,t) = 1$ et ceci contredit l'existence de p. Par conséquent $t = \pm 1$ et $x \in \mathbb{Z}$.

q4) A priori $c \in \mathbb{Q}$ puisque u ou v est négatif. Mais comme $c^{25} = a \in \mathbb{N}$, d'après la q3) on a $c \in \mathbb{Z}$. On a aussi c non nul car a non nul, et c positif car a positif donc $c \in \mathbb{N}^*$. On aurait pu utiliser également $c^9 = b \in \mathbb{N}$ pour aboutir aux mêmes conclusions.

q5) D'après le théorème de Bezout on sait qu'il existe $(u,v) \in \mathbb{Z}^2$ tel que $nu + mv = 1$. Pour $c = a^u b^v$ on a

$$c^n = a^{nu} b^{nv} = a^{nu} a^{mv} = a \quad \text{et} \quad c^m = a^{mu} b^{mv} = b^{nu+mv} = b$$

A priori $c \in \mathbb{Q}$ mais comme $c^n = a \in \mathbb{N}^*$ on a d'après q3) que $c \in \mathbb{Z}$ et $c \neq 0$. Si n est pair, m est impair car $\mathrm{pgcd}(m,n) = 1$ donc $c^m = b > 0$ nous aide à conclure que $c \in \mathbb{N}^*$. Si n est impair on a $c^n = a > 0$ donc de nouveau $c \in \mathbb{N}^*$. Dans tous les cas $c \in \mathbb{N}^*$.

Pour cet exercice on aurait pu utiliser aussi la décomposition en facteurs premiers de a et de b :

Si $a = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$

$b = p_1^{\beta_1} \cdots p_s^{\beta_s}$ avec $\alpha_i \geq 0, \beta_i \geq 0$ et p_i les facteurs premiers de a et de b alors la décomposition de

$x = a^m = b^n$ et $\prod_{i=1}^{s} p_i^{m\alpha_i} = \prod_{i=1}^{s} p_i^{n\beta_i} = x$ et par unicité

on a $m\alpha_i = n\beta_i$ $\forall i$ de 1 à s. Or $m \mid n\beta_i$ et $\text{pgcd}(m,n) = 1$ implique par le lemme de Gauss que $m \mid \beta_i, \forall i$.

De même $n \mid m\alpha_i$ $\forall i$ et $\text{pgcd}(m,n)=1$ implique que $n \mid \alpha_i, \forall i$.

Donc $\alpha_i = n\alpha_i'$, $\beta_i = m\beta_i'$ $\forall i$ et $mn\alpha_i' = mn\beta_i'$ donc $\alpha_i' = \beta_i'$.

Alors $a = \left(\prod_{i=1}^{s} p_i^{\alpha_i'}\right)^n = c^n$ pour $c = \prod_{i=1}^{s} p_i^{\alpha_i'}$ et

$$b = \left(\prod_{i=1}^{s} p_i^{\alpha_i'}\right)^m = c^m \quad \text{et } c \in \mathbb{N}^*.$$

Remarque. Cet exercice et le ~~petit~~ théorème de Fermat ($x^{p-1} \equiv 1 \ [p]$ si p premier, $p \nmid x$) nous permettent de résoudre d'une autre manière l'exercice 26 :

Comme $n = a^2 = b^3$ et que $\text{pgcd}(2,3) = 1$ on a que $a = c^3$ (et $b = c^2$) donc $n = c^6$. Si $7 \mid c$ alors $7 \mid c^6 = n$ donc $n = 7k$ pour $k \in \mathbb{N}$.

Si $7 \nmid c$ on applique le petit théorème de Fermat avec $p = 7$ premier. Donc $n = c^{7-1} = c^6 \equiv 1 \ [7]$ d'où $n = 7k+1$ pour $k \in \mathbb{N}$.